

Forensic Smartphone Analysis Using Adhesives: Transplantation of Package on Package Components

Th. Heckmann^{a,b,c}, K. Markantonakis^b, D. Naccache^c, Th. Souvignet^a

^a*Institut de Recherche Criminelle de la Gendarmerie Nationale, Digital Forensics Department (INL), 5, boulevard de l'Hautil, 95300 Cergy-Pontoise, France*

^b*Royal Holloway, University of London, Information Security Group Smart Card and IoT Security Centre, Egham, Surrey, TW20 0EX, United Kingdom*

^c*Ecole Normale Supérieure, Information Security Group, Computer Science Department, 45, rue d'Ulm, 75230 Paris, France*

Abstract

Investigators routinely recover data from mobile devices. In many cases the target device is severely damaged. Events such as airplane crashes, accidents, terrorism or long submersion may bend or crack the device's main board and hence prevent using standard forensic tools. This paper shows how to salvage forensic information when NAND memory, SoC or cryptographic chips are still intact. We do not make any assumptions on the state of the other components. In usual forensic investigations, damaged phone components are analysed using a process called "forensic transplantation". This procedure consists of unsoldering (or lapping) chips, re-soldering them on a functional donor board and rebooting.

Package on Package (PoP) component packaging is a new technique allowing manufacturers to stack two silicon chips, e.g. memory, CPU or cryptographic processors. Currently, PoP is widely used by most device manufacturers and in particular by leading brands such as Apple, BlackBerry, Samsung, HTC and Huawei. Unfortunately, forensic transplantation destroys PoP components.

This work overcomes this difficulty by introducing a new chip-off analysis method based on High Temperature Thixotropic Thermal Conductive Adhesive (HTTTCA) for gluing the PoP packages to prevent misalignment during the transplantation process. The HTTTCA process allows the investigator to safely unsolder PoP components, which is a crucial step for transplantation. To demonstrate feasibility, we describe in detail an experimental forensic transplantation of a secure mobile phone PoP CPU.

© 2018 RHUL/ENS/IRCGN

Keywords: Forensic Rework, Hardware Forensics, Adhesives Properties, Forensic Transplantation.

Introduction

Forensic investigators must frequently bypass the protections of embedded systems to access digital evidence. Terrorism and mass accidents¹ are on the increase and the analysis of mobile devices is necessary to address various needs: legal (proof in court), technical (understanding the disaster) and ethical (mourning of the victims' families).

This paper concerns the recovery of data from damaged smartphones. The damage levels considered in our setting can be severe: we assume that the main boards might be broken or

severely bent, but that the NAND, SoC or cryptographic chips remain intact. As of today, the mobile phone industry largely uses a new packaging technology called Package on Package (PoP). Miniaturisation and the race for performance and security make PoP omnipresent. Indeed, PoP is deployed in the latest smartphone generations: iPhone X, iPhone 8, iPhone 8 Plus (A11 Bionic PoP), iPhone 7, iPhone 7 Plus (A10 Fusion processor APL1W24 PoP), iPhone 6S Plus (A9 processor PoP), BlackBerry 9900 (Qualcomm 8655 PoP processor), BlackBerry Z10 (Qualcomm Snapdragon S4 Plus processor PoP), Samsung Galaxy S7 edge (Qualcomm 820 Snapdragon or Samsung Exynos 8890), HTC 10 (Snapdragon 820), Huawei Mate 8 (Kirin 950), etc. Unfortunately, unsoldering PoP components for transplantation is extremely difficult using traditional techniques.

This paper shows how specific adhesives (thermally conductive and electrically insulating epoxy) can allow the investigator to unsolder PoP components without destroying them including cases when the PoP stack solder balls have the same or

Email addresses:

thibaut.heckmann@gendarmerie.interieur.gouv.fr (Th. Heckmann), K.Markantonakis@rhul.ac.uk (K. Markantonakis), david.naccache@ens.fr (D. Naccache),

thomas.souvignet@gendarmerie.interieur.gouv.fr (Th. Souvignet)

¹e.g. the attacks in Paris [1], Nice [2], the Germanwings crash [3] and the Puisseguin bus accident [4].

similar liquidus temperature as the PCB soldering material. We call the new process PoP TCA Chip-Off (TCACO). To illustrate this work, we describe a step-by-step TCACO transplantation of a PoP CPU in a BlackBerry 9900 PGP.

1. Traditional mobile device forensic techniques

To analyse a fully functional phone [5], forensic investigators create a physical memory dump of the device and then extract from the dump call information, SMS, MMS, videos, photos and phone book, as well as data deleted by the user (but still present in the unallocated memory space). In most cases, devices are connected to a forensic analysis device via a USB cable connection [6]. The analysis tool communicates with the phone to extract data [7]. To that end, judicial investigators often use devices (software suites and hardware) specially developed by firms, such as Cellebrite UFED [8], Micro Systemation XRY [9], Oxygen Forensic Suite [10], etc. When commercial equipment does not support a specific mobile device, forensic investigators develop their own programs (which requires development effort) or use the method developed in [11].

2. Traditional forensic techniques for damaged mobile devices

Damaged (unresponsive) mobile phones cannot be connected via cable connection to off-the-shelf analysis devices. To extract data from damaged phones, investigators use specialised flashing tools [12] initially designed to repair mobile devices (RIFF Box, Octoplus, Medusa Box, etc.). Such flashing tools use the JTAG [13] interface (JTAG is normally used to test or debug embedded systems but can also be used to access flash memory [14]). Finally, if extraction via JTAG is impossible, flash memory chip de-soldering and reading [15] must be used (chip extraction, reading data from the memory chip, followed by a manual or automated flash translation layer (FTL) reconstruction). However, with the arrival of phones featuring internal memory encryption, traditional chip-off techniques are no longer sufficient to analyse damaged phones. Forensic transplantation becomes the only means to recover data.

3. What is a forensic transplantation ?

Forensic transplantation (Fig. 1) consists in taking electronic components from a defective phone [16] and re-soldering them into a functional one. The process is analogous to human organ transplantation. A healthy organ (processor and memory of the damaged board) in a failing body (damaged main board) is transplanted to replace a failing organ in a healthy body (donor board). The functional phone board is called a *donor board*. The preparation of the donor board is an essential step in removing components from it without damaging the board (usually during this operation components are destroyed by lapping or chip-off). In parallel, the components of the *damaged board* are removed and then re-soldered on the donor board. Once these two steps are completed, all that remains is to turn on the

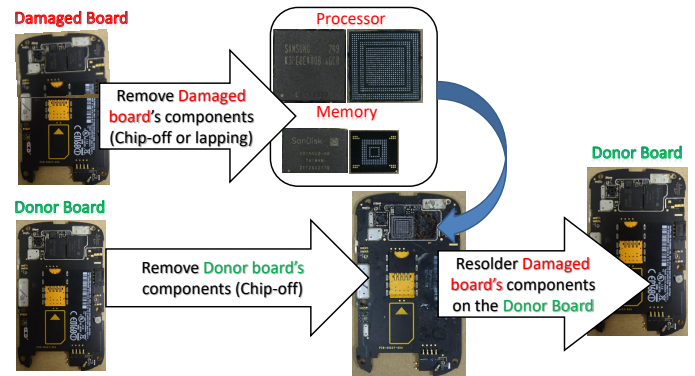


Figure 1: Transplantation principle

phone and analyse it. This allows the investigator to retrieve the data (or bypass some security mechanism) that could serve as evidence in court.

Similarly, other transplantation methods [17] allow the reading of the volatile memory (DRAMs retain their contents for several seconds after power-off). A typical example is the “cold boot attack” that involves cooling memory chips using liquid nitrogen and transplanting them into a donor device capable of reading those chips [18]. Thus, we can use forensic transplantation to extract and analyse data present in a damaged device, whether the memory medium is volatile or not.

4. What is a Package on Package component?

Package on Package (PoP) is a semiconductor packaging process (Fig. 2²) consisting of the stacking of two or more dies (memory die, CPU die, RAM, etc.) on top of one another.

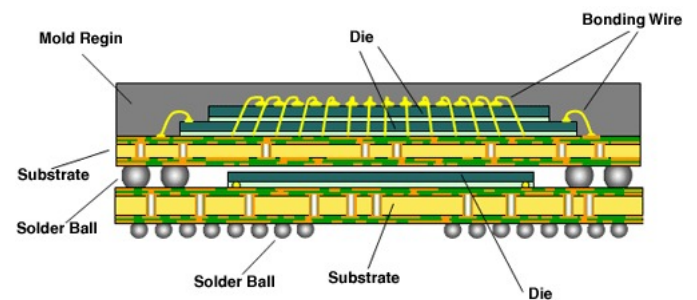


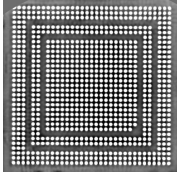
Figure 2: Package on package component principle

The PoP technology combines two or more BGAs (Ball Grid Arrays) into a vertically stacked component. Manufacturers are now increasingly deploying this technology:

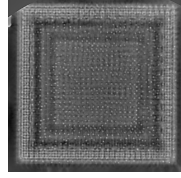
- BlackBerry 9900 (Fig. 3) uses a Single core, 1200 MHz, QC 8655 CPU stacked on top of a 0.75 GB RAM;
- BlackBerry Z10 (Fig. 4a) uses Qualcomm MSM8960 Snapdragon S4 Plus, Dual-core 1.5 GHz Krait CPU stacked on top of a 2 GB RAM;

²<https://electronics.stackexchange.com>

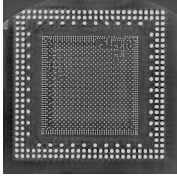
- Apple iPhone 6S uses A9 APL0898 processor and DRAM (Micron) D9SND (MT53B256M64D2NL); iPhone X uses APL1W72 A11 (also used in the iPhone 8 and 8 Plus), layered over SK Hynix 3 GB LPDDR4x RAM.
- Samsung S7 edge (Fig. 4b) uses Qualcomm Snapdragon 820 processor and SK Hynix H9KNNNCTUMU-BRNMH 4 Go LPDDR4 SDRAM.



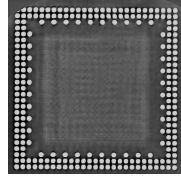
(a) Bottom CPU BGA on PCB



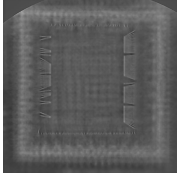
(b) CPU via connection



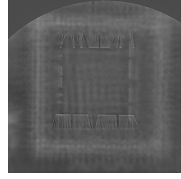
(c) CPU and RAM junction



(d) RAM BGA on the CPU

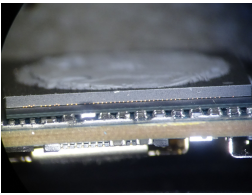


(e) middle RAM bonding wires

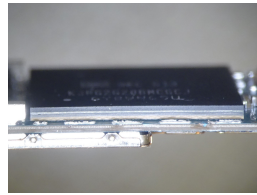


(f) Top RAM bonding wires

Figure 3: BlackBerry 9900 PoP CPU X-ray images



(a) BlackBerry Z10: PoP CPU (bottom) and RAM (top)



(b) Samsung S7 edge: Qualcomm PoP processor

Figure 4: BlackBerry and stacked CPUs

air flux, heats the top of the component while a plate heats the board. Once the balls' melting temperature has been reached, the component is unsoldered with a vacuum pump (Fig. 5).

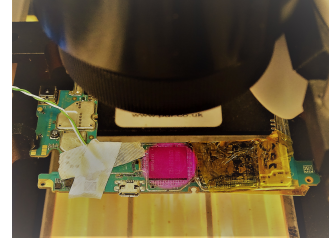
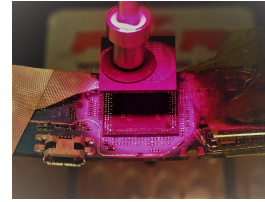
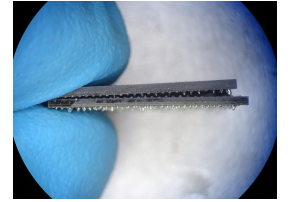


Figure 5: BGA station: CPU unsoldering

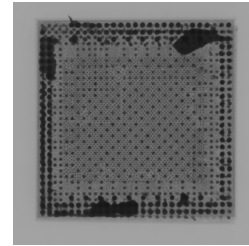
However, the technique is limited because it can lead to the destruction of the PoP component (Fig. 6a and 6b). Because when the liquefaction temperature is reached, the stacked balls are destroyed.



(a) BGA station: stack destruction



(b) BlackBerry Z10 PoP CPU: CPU (bottom) and RAM (top)



(c) BlackBerry Z10 PoP CPU after chip-off (X-ray image)

Figure 6: Chip-off PoP CPU destruction

Moreover, the mechanical forces (Equation 1 [20] and Fig. 7) exerted are too high due to the thermal expansion coefficient $\Delta\alpha$, and the temperature difference applied ΔT . This coefficient represents the relative change in linear dimensions, per unit of temperature change:

$$curvature = \frac{2 \sin \tan^{-1}(\frac{\delta}{x})}{\sqrt{x^2 + \delta^2}} \text{ with } \Delta\delta = \Delta\epsilon \cdot \Delta T \quad (1)$$

Those forces create false internal contacts, making the component unusable (Fig. 6c).

5.2. Lapping machine

A second commonly used technique is “lapping” (Fig. 8). The PCB is first cut mechanically around the component to be

5. Traditional techniques and their limits

5.1. High temperature chip-off

Chip-off is a technique where a component is physically removed from the device and examined externally [15]. In some cases, it may be necessary to use the chip-off technique to obtain a memory image or to reverse engineer a secure mobile device [19]. For BGA components, the use of a BGA unsoldering station is often preferred. An infrared beam, or a hot

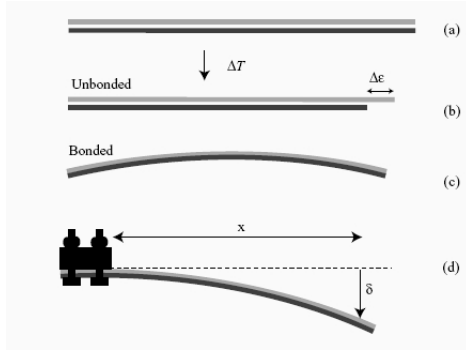
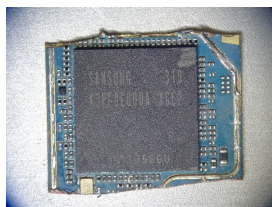
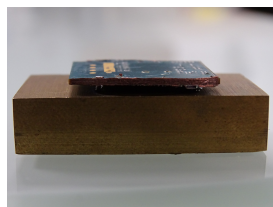


Figure 7: Bonded materials and mechanical forces due to temperature difference

extracted (Fig. 8a). Next, the component is glued, using an adhesive, onto a perfectly flat metallic support (Fig. 8b). The different layers constituting the PCB are then sanded (Fig. 8c) and removed one by one as shown in (Fig. 8d, 8e, 8f and 8g). Finally, once the last layer is removed, the component is cleaned using a soldering iron and flux remover (Fig. 8h).



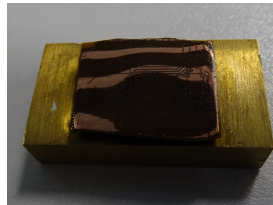
(a) BlackBerry PCB cutting



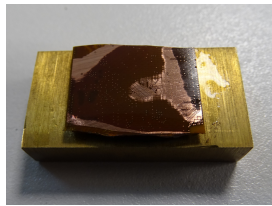
(b) CPU before lapping



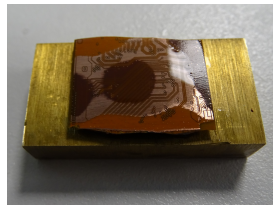
(c) Manual lapping



(d) 3 minutes' lapping



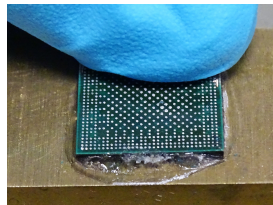
(e) 6 minutes' lapping



(f) 9 minutes' lapping



(g) 12 minutes' lapping



(h) CPU cleaning after 15 minutes' lapping

Figure 8: Lapping process steps

With new generations of phones, the limit of this technique has been reached. If we take the BlackBerry Z10 or the iPhone 5 as examples, the memory component is located just behind the PoP processor (Fig. 9).

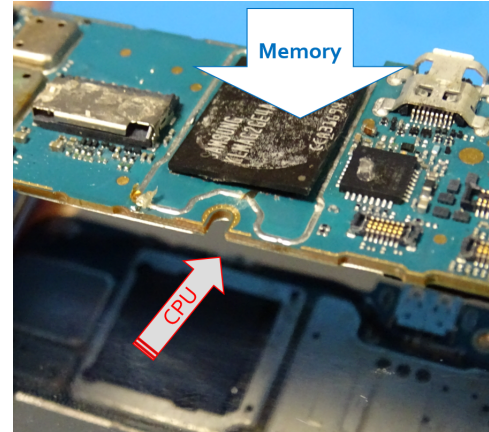


Figure 9: BlackBerry Z10: Memory and CPU mirroring

Therefore, traditional lapping leads to the destruction of either the PoP CPU or the memory component. As the two components must be transplanted to make the phone usable again, this technique is inappropriate.

6. Material

6.1. High Temperature Thixotropic Thermal Conductive Adhesive

Generally, this adhesive covers memory components and CPUs to reduce chip heating because this polymer family is designed to dissipate heat [21] [22]. It also improves sturdiness, which makes chip-off analyses considerably more difficult (the curing temperature is an additional stress to the chip).

The thermal conductive adhesive studied in this paper (Polytec TC430³) consists of two components: resin and hardener. The mixing ratio is 100 resin units by weight for 4 hardener units (Fig. 10).

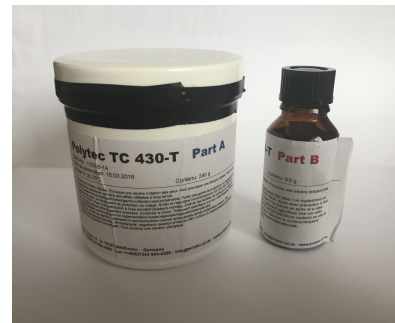


Figure 10: HTTCA resin, left; hardener, right

³http://www.polytec-pt.com/fileadmin/user_uploads_Polytec-PT/home/documents/Polytec_Klebstoffe_ENG/Polytec_TC_430_eng1.pdf

Viscosity at 23 °C is 13000 mPa · s and minimum bond line cure schedule is 60 minutes at 100 °C and 15 minutes at 150 °C. The pot lifetime at 23 °C is 2 days, which allows making alterations. The degradation temperature is 400 °C. The fundamental importance of this data will be discussed later. Another interesting property is that TC430 is a thixotropic consistency paste. So, under constant stress (or gradient of velocity), its apparent viscosity decreases with time. Therefore, TC430 will not expand as the temperature increases, which is a major advantage in the transplantation of PoP components.

7. PoP chip-off/TCA method

7.1. Applied method

The new PoP chip-off/TCA method will now be described. This process is necessary for transplantation when there are no other ways to de-solder PoP components. The process is broken down into steps as follows:

- Step 1: Identification of the components that need to be transplanted. Indeed, it is not necessary to transplant all the components: only as many of them as necessary. As described in section 8, before any transplantation it is necessary to understand the phone's security mechanisms using hardware/software reverse engineering.

When a phone containing evidence is damaged, many small electronic components can be the cause of the malfunction requiring the forensic transplant. To minimise the risk of transplanting defective electronic components, it is necessary to transplant only the components essential to recover the forensics data (memory components, CPU, cryptographic chips).

- Step 2: X-ray tomography is performed to verify that the components to transplant are not destroyed, to check that all bonding connections are undamaged (Fig. 11), and that there is no silicon fracture.

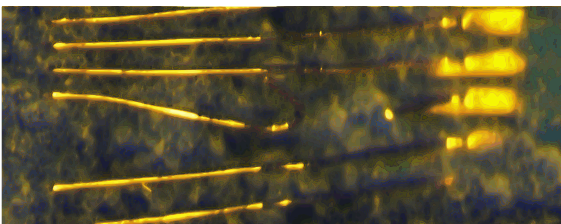


Figure 11: eMMC memory broken bonding wire

In forensic cases (crash, accident, terrorist incidents), this step is often essential because the verification of the component's physical state makes it possible to avoid irreversible destruction (and thus loss of data) typically due to a broken bonding wire (false contact) or to silicon weakened during an impact.

- Step 3: The HTTTCA (High Temperature Thixotropic Thermal Conductive Adhesive) is applied to the stack

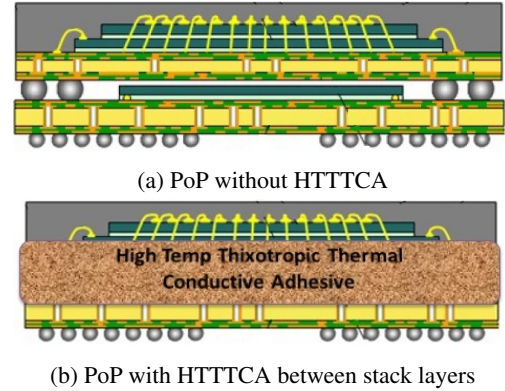
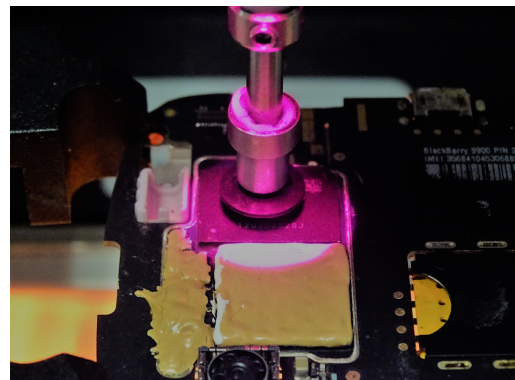


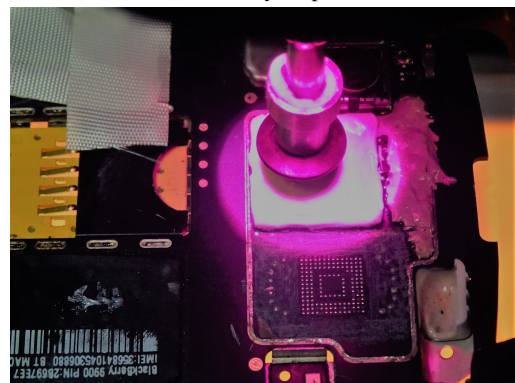
Figure 12: Application of the HTTTCA

(between the RAM and the CPU) (Fig. 12) using a micro-tool. Once the adhesive has been applied, it must dry according to the manufacturer's data. Because the glue is thixotropic, it will not expand during the drying process. There is therefore no risk of damaging the stacks and destroying the electronic components.

- Step 4: A classic unsoldering process (chip-off) [15] is applied to all the necessary components to be transplanted (Fig. 13). The components required for forensic transplantation are those determined at the end of Step 1.



(a) Memory chip-off



(b) PoP processor chip-off

Figure 13: Chip-off

- Step 5: The investigator must check that the PoP is stable using X-ray tomography (Fig. 14). The main advantage of the technique proposed in this paper is the ability to realise the chip-off technique without creating false contacts between the balls and between the PoP's different levels. This step is essential to verify that the technique has been performed correctly.

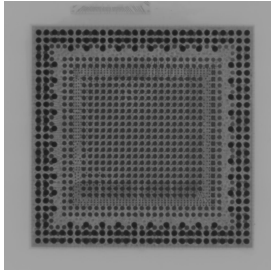
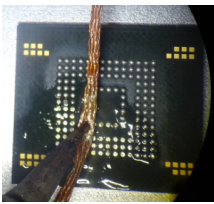
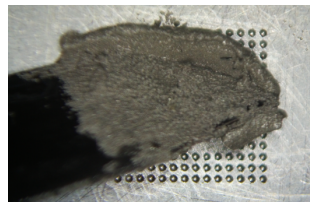


Figure 14: X-ray control to check that the stacked component did not move

- Step 6: The chip is cleaned (Fig. 15a) using a soldering iron and flux remover. Once this is done, the low-temperature re-balling process is applied (Fig. 15b) [23].



(a) Chip clean-up



(b) Low-temperature re-balling process

Figure 15: Step 6: clean-up and re-balling process

It is advisable to solder with a low-temperature paste to minimise the thermal shock applied to the electronic component. Re-soldering with a high-temperature paste is possible but riskier and may potentially damage the component. It is important to bear in mind that it has already undergone a major shock during an incident and must be considered as already fragile.

- Step 7: The donor board is prepared by removing the necessary components determined in Step 1. The main board's components will be soldered (Step 9) in its PCB's gap positions. The components can be removed (Fig. 16) either by de-soldering using the conventional chip-off technique, or by milling. This step is important because no other donor board components should be damaged. The choice of the proper method must be reflected upon carefully to prepare a perfect donor board. Thus, in the case of heat-sensitive components, the milling method is preferable. However, when components are located in a high density area and are sensitive to mechanical stress, the chip-off technique would be preferable.
- Step 8: The main board's components are attached, using



Figure 16: Donor board eMMC gap position

a low-temperature method, onto the donor board using a BGA station (Fig. 17) or manually.

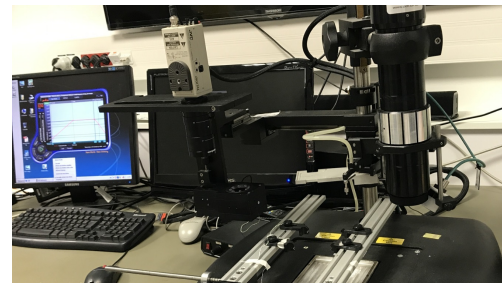


Figure 17: Re-work with a BGA station

- Step 9: X-ray tomography is used to verify that the components are well soldered on the donor board and check that there are not false electrical contacts between balls (Fig. 18).

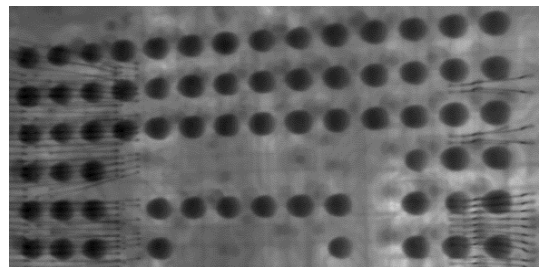


Figure 18: X-ray confirmation of donor board soldering

This step verifies that each ball is properly soldered. Otherwise an uncorrelated ground output may destroy the component, as would a short circuit.

- Step 10: Finally, the donor phone's other components are set up (screen, keyboard, etc.) and the device turned on for forensic investigations. This stage confirms the successful completion of the forensic transplant. If this step is satisfactory, Step 1 will no longer need to be carried out for future devices of the same model phone (or GPS, etc.).

However, if Step 1 has been incorrectly performed, the phone will not boot, or anomaly indicators will appear (blue screen or others). These indicators reflect the fact that all the necessary components have not been properly transplanted (e.g. cryptographic chips, CPUs, memories, etc.). Finally, if the phone still does not boot even if step 1 is performed correctly, the investigator must look more closely at Step 2 to find the malfunction. If the defective component is an essential component as per Step 1, then it will be impossible to perform the forensic transplant.

8. Direct forensic application: BlackBerry 9900 PGP

8.1. BlackBerry 9900 PGP cryptography

The first step is to select the components to be transplanted. Hence, it is essential to understand the encryption mechanisms used in the BlackBerry 9900 (Fig. 19). These are described on BlackBerry's website [24].

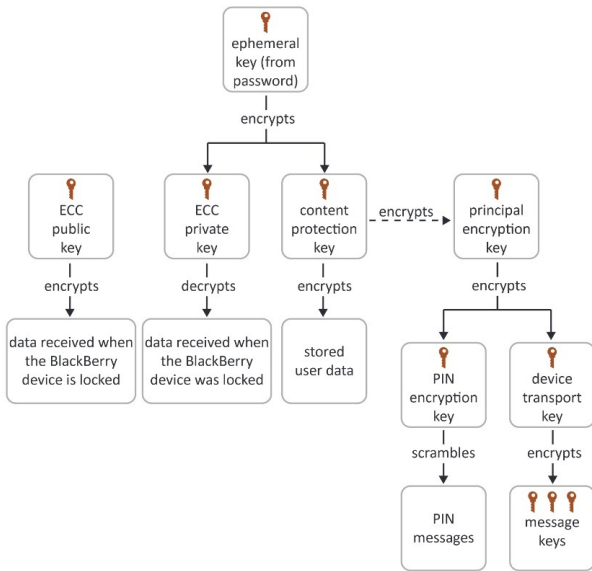


Figure 19: BlackBerry key hierarchy [24]

The Hardware Encryption Key (K_{hard}) is etched in the CPU's silicon, but cannot be physically accessed (by reading). K_{hard} is, in a way, a master key encrypting a container containing an Ephemeral Key (K_{eph}). K_{eph} is derived from the unlocking password entered by the user and encrypts the ECC (Elliptic Curve Cryptography) private key (K_{ECC}) and the device's Content Protection Key (K_{cp}). K_{cp} allows the investigator to access user data when the device is locked.

8.2. BlackBerry 9900 transplantation

- Step 1: The study confirms that the processor (containing the Hardware Encryption Key (K_{hard})) and the memory component (containing the encrypted user data and enabling decryption) are the only two components to be transplanted (Fig. 20).

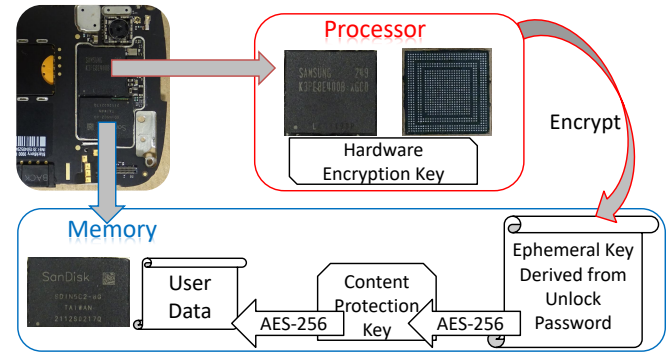


Figure 20: Simplified BlackBerry Encryption Process

- Step 2: The two main board components are then X-rayed to check that they are undamaged (Fig. 21). In this case, X-ray control reveals that components seem operational, hence we can move on to the next step.

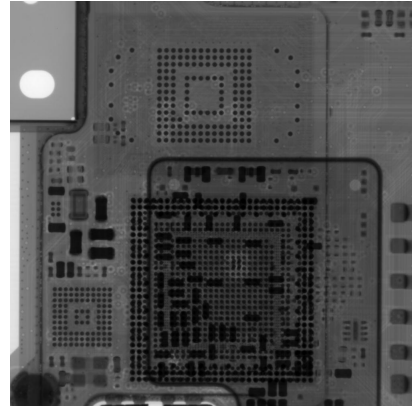


Figure 21: BlackBerry 9900 PoP CPU and memory X-ray soldering control

- Step 3: A High Temperature Thixotropic Thermal Conductive Adhesive (Polytec TC430-T) is then applied (Fig. 22) with a micro-tool from Ted Pella, Inc.⁴ Then, if any underfill is present, it can be removed to better apply the adhesive (Fig. 22c). As soon as the four sides are glued (Fig. 22e), the adhesive is left to dry (60 minutes at 100 °C or 15 minutes at 150 °C).
- Step 4: The PoP CPU and the memory are then de-soldered using chip-off method (Fig. 23). The BlackBerry 9900 phone has underfill under the processor and memory component. It is advisable to use the micro-cutting instrument to facilitate the destruction of underfill glue. Since the temperature is important during the movement of the instrument, it is advisable not to carry out a pivot movement which could destroy the component. The micro-instrument is used by performing only horizontal micro-movements, which will remove the underfill excess and

⁴https://www.tedpella.com/tools_html/micro-tool-overview.htm

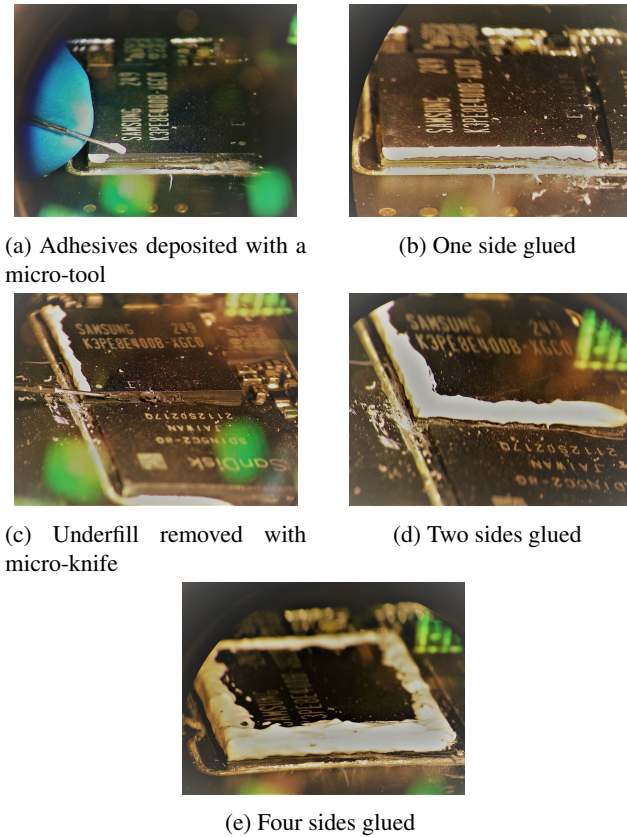


Figure 22: Step 3: Adhesive deposit around the stack PoP CPU

thus facilitate the unsoldering of the electronic component. As the degradation temperature of the TC430-T is much higher than the industrial underfill, the stack does not move and the PoP remains in perfect condition.

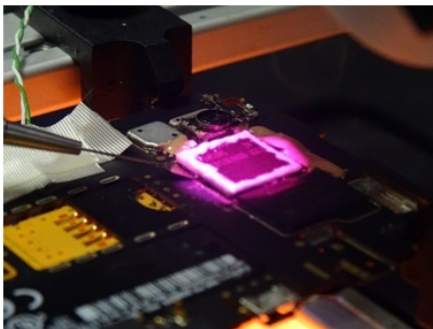


Figure 23: BlackBerry 9900 PoP CPU unsoldering using chip-off/TCA technique

- Step 5: X-ray tomography is then performed to confirm that the technique has not damaged the stacked component. Each of the balls must be checked to confirm that there is no migration or unwanted junction of balls.
- Step 6: The low-temperature reballing technique is then applied [23] (Fig. 24). The masks are custom-made and they must perfectly fit the electronic component to be re-balled. As has been studied in [23], the thickness of the

mask is an important datum that will play a crucial role in the quantity of material used and therefore the thickness of the ball. Thus, for the re-balling of a CPU, with a high density of balls, the thickness of the mask (127 micrometres) will be less than for a memory mask (152 micrometres).

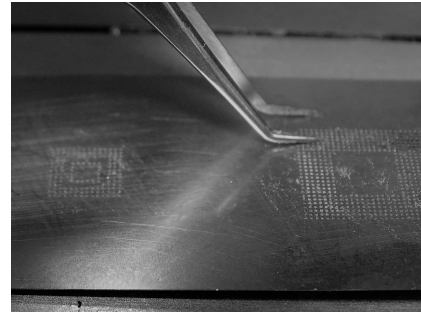
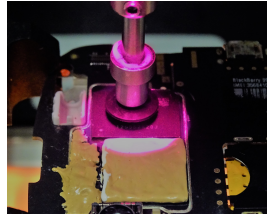


Figure 24: Re-balling process using stencil

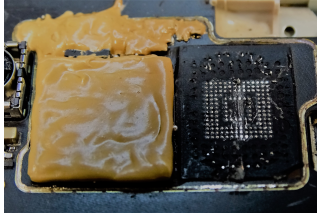
- Step 7: The donor board is then prepared (Fig. 25). In order not to risk damaging the micro-electronic components located on the periphery of the memory and the CPU (capacitors, etc.), it is first necessary to deposit high-temperature thixotropic adhesive (Fig. 25a). As much as possible, the donor board must be protected from the risks of thermal or mechanical shock applied while unsoldering and soldering. Then unsoldering can be performed at 290 °C using a micro-instrument in order to remove the underfill and facilitate the process (Fig. 25b). A micro-cutting instrument and a heated micro-pane are used jointly to remove the underfill residues remaining on the board (Fig. 25d and 25e). The same process for the processor is used (Fig. 25f and 25g). As the processor soldering balls are smaller than the memory ones, it is necessary to be even more careful when cleaning the board. Indeed, the risk here is tearing off tracks present on the PCB and thus destroy the donor board. After a final wash with flux remover, the donor board is ready to accommodate the main board components (Fig. 25h).
 - Step 8: The CPU and the memory (from the damaged board) are soldered onto the donor board, using a BGA station at low temperature (150 °C).
 - Step 9: X-ray radiography is performed to check that the CPU and the memory have been properly soldered (Fig. 26). If the X-ray shows that there are no false contacts between the balls and that the balls are properly soldered, the investigator can move to the next step.
- If there are false contacts, the component must be unsoldered, cleaned, re-balled at low temperature and resoldered on the donor board. A new check radiograph is then taken. If radiography does not reveal any issues, then we can move on to the next step. Otherwise, the process must be repeated.



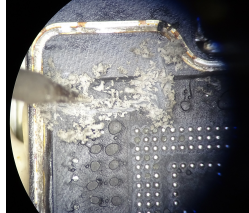
(a) Protecting the donor board with adhesive



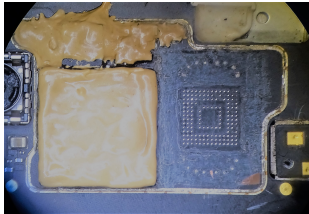
(b) Memory unsoldering



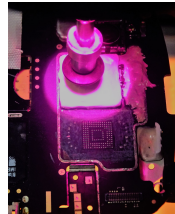
(c) Memory underfill



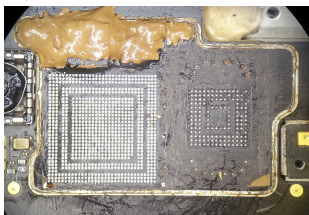
(d) Underfill removed with micro-pane



(e) Cleaned donor board memory location



(f) Processor unsoldering



(g) Cleaned donor board processor location



(h) Donor board ready to accommodate the main board's components

Figure 25: Step 7: Donor board preparation

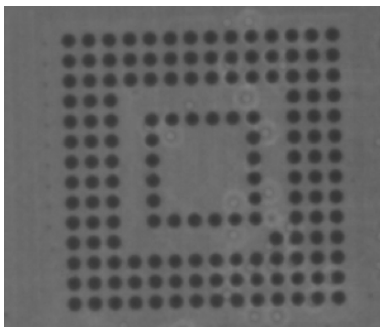


Figure 26: Check X-ray of eMMC position with good soldering

- Step 10: If all previous steps have been correctly performed, the phone components (keyboard, screen, battery, etc.) can be inserted and the phone switched on. The

phone should start properly on its boot sector (Fig. 27). The forensic transplant is thus successful on this BlackBerry 9900 phone.



Figure 27: Post transplantation BlackBerry 9900 reboot

If Step 10 is correct, the investigator is now able to use traditional forensics techniques to extract and analyse data from this undamaged mobile device.

9. Discussion

9.1. Choice of adhesives and limits

At present, phone manufacturers use glue that degrades at about 300 °C. They use this adhesive to facilitate the thermal diffusion of their components. It provides a means of protection against heat and thus increases components' robustness and long-term reliability.

At the time of writing this paper, manufacturers do not use glue with a degradation temperature higher than 300 °C, as it does not provide an additional thermal advantage for them. The key idea in this paper was to use an HTTTCA adhesive with a degradation temperature higher than 300 °C. Thus, it would be possible to investigate the limits of our method, if manufacturers were to use even higher temperature adhesives. We could find an initial solution by putting between the dies of the PoP component an even higher temperature glue. However, it would be necessary not to neglect the effect of the higher temperature of unsoldering which would surely destroy the PoP component. This component could be covered with a powerful heat skin and heat applied to the PCBs copper layers at a higher temperature.

9.2. Quality assurance of the process

Quality assurance is an important step throughout the process we have developed in order to preserve data in a forensic framework. In order to improve the reliability and repeatability of our procedure, we needed to perform the test on a reference

device (of the same model). In the same way, in order to improve the traceability, it was also important to save the reflow profile, and also if possible, the temperature monitoring measurements of the experiments. In this sense, as we have seen in the various steps of our process, radiotomography control is an important step in order to avoid any risk of short circuit which is likely to destroy the memory chip (with the user data and user password) or processor (with the encryption key). We note, however, that the process we have developed requires that the component be heated to a high temperature, which constitutes a possible risk of data corruption that the investigator would have to take into account before carrying out this crucial step. It is for this reason that we opted for reballing and resoldering of the component at low temperature to minimize the risk of thermal shock during resoldering operations. Still in this quality assurance framework, it could even be possible to use conductive glue that dries at room temperature to recreate the beads, and then in a second step, glue the electronic component directly to the PCB at room temperature to further eliminate the risk of thermal shock.

Finally, we note in step 3 of our method that the application of the glue is performed manually. For more precision, this deposit could be made with a time-pressure device specifically designed to do micrometric gluing, such as Nordson Performus II.



Figure 28: Nordson Performus II pump

9.3. For which other devices is transplantation applicable ?

We have seen in this paper an example of application of the method for encrypted mobile phones. The method can also be used on any damaged device having a memory encrypted by a processor or crypto-component, such as GPS, tablet, etc. On non-encrypted devices, the transplantation, as well as the proposed method, have only minor interest, since the simple reading of the memory is sufficient to extract the data for analysis. In this case, if an unencrypted device is damaged, the layer-by-layer lapping method would be preferable and much quicker to implement on PoP memory components. Moreover, in the interests of quality assurance, the lapping technique would not subject the component to a high temperature risk, especially on components which had already suffered a shock.

9.4. Which electronic components should be transplanted?

Also transplantation can be a long process depending on the number of components to be transplanted. It is not a ques-

tion of transplanting all the components, but of making a rigorous selection. To understand the security mechanisms inside the phone, reverse engineering of the components must be executed, before the transplantation test.

On phones that have a low security level (no encryption), the only component to be transplanted may be the memory.

However, as we have just seen, in phones with embedded encryption, such as the BlackBerry, the presence of hardware encryption keys in the processor requires the transplantation of both the memory and the processor.

Finally, in the case of some manufacturers (Apple for example), it is necessary to identify the components that are paired inside the phone. We first have to understand the components that need to be transplanted: memory, processor and the ID crypto-components that are used.

9.5. Transplantation limits

It has been seen that transplantation is impossible if the memory component and/or the CPU and/or cryptographic chip are damaged (broken silicon). Thus, before any transplantation, the essential components to be transplanted must be X-rayed to diagnose the origin of the problem and proceed to the component's repair (bonding repair, etc.).

10. Conclusion and further research

10.1. First results

The transplantation of the current generation of mobile phones is a very complex operation entailing a risk of PoP components' destruction. The goal of this paper is to propose a new method called "PoP chip-off/TCA Technique" allowing the desoldering of PoP components without damaging them, and generally ensuring a more successful transplantation in present-day mobile phones. We describe the current methods used for transplanting phones and their limitations.

Finally, a new method has been developed and successfully applied to the forensic transplantation of a cryptographic BlackBerry 9900 PGP mobile phone.

10.2. Future developments

Unlike BlackBerry or Samsung devices, the transplantation of Apple devices (iPhone 6S, iPhone 7, iPhone 8, and iPhone X) is challenging because crypto-chips are paired inside the phone's board (not only memory and CPU). Hence it would be necessary to learn more about the crypto-chips paired inside these systems (baseband processor, touch ID, anti-rollback EEPROM and baseband flash), and then use the adhesives techniques to desolder and solder the Apple Package on Package (PoP) components to proceed with an iPhone 6S or an iPhone 7 transplantation. This is the area of the authors' current research.

Acknowledgements

The authors thank Graham Houghton and Dame Natacha Laniado for their support, proofreading and contribution to this article.

- [1] BBC-News-1, Paris attacks: Key questions after Abaaoud killed, [online] <http://www.bbc.com/news/world-europe-34866144> (2015). URL <http://www.bbc.com/news/world-europe-34866144>
- [2] BBC-News-2, Nice attack: At least 84 killed by lorry at Bastille Day celebrations, [online] <http://www.bbc.com/news/world-europe-36800730> (2016). URL <http://www.bbc.com/news/world-europe-36800730>
- [3] BBC-News-3, Germanwings crash leaves unanswered questions, [online] <http://www.bbc.com/news/world-europe-32084956> (2017). URL <http://www.bbc.com/news/world-europe-32084956>
- [4] BBC-News-4, Bus crash kills at least 42 in Gironde region of France, [online] <http://www.bbc.com/news/world-europe-34612720> (2015). URL <http://www.bbc.com/news/world-europe-34612720>
- [5] R. Van Der Knijff, Embedded systems analysis, in: Chapter 11 of Handbook of Computer Crime Investigation: Forensic Tools and Technology, E. Casey (Ed.), 2002.
- [6] A. Hoog, in: Android Forensics: Investigation, Analysis and Mobile Security for Google Android, Syngress Publishing, 2011.
- [7] R. Ayers, in: An overview of cell phone forensic tools, NIST, 2006.
- [8] Cellebrite, UFED ultimate, <https://www.cellebrite.com/en/products/ufed-ultimate/> (2017).
- [9] XRY-Micro-Systemation, XRY physical for forensic applications, <https://www.msab.com/products/xry/xry-physical/> (2017).
- [10] Oxygen, Oxygen forensic suite, <https://www.oxygen-forensic.com/en/> (2017).
- [11] R. Ayers, S. Brothers, W. Jansen, in: Guidelines on Mobile Device Forensics, NIST, 2014. doi:<http://dx.doi.org/10.6028/NIST.SP.800-101r1>.
- [12] K. Jonkers, The forensic use of mobile phone flasher boxes, Digital Investigation 6 (3) (2010) 168–178, Embedded Systems Forensics: Smart Phones, GPS Devices, and Gaming Consoles. doi:<http://dx.doi.org/10.1016/j.diin.2010.01.006>. URL <http://www.sciencedirect.com/science/article/pii/S1742287610000083>
- [13] IEEE, Computer society, Standard test access port and boundary-scan architecture (2013).
- [14] M. Breeuwsma, Forensic imaging of embedded systems using jtag (boundary-scan), Digital Investigation 3 (1) (2006) 32–42. doi:<http://dx.doi.org/10.1016/j.diin.2006.01.003>. URL <http://www.sciencedirect.com/science/article/pii/S174228760600003X>
- [15] M. Breeuwsma, M. De Jongh, C. Klaver, R. Van Der Knijff, M. Roeloffs, Forensic data recovery from flash memory, Small Scale Digital Device Forensics Journal 1 (1) (2007) 1–17.
- [16] I. Androulidakis, Mobile phone security and forensics, Springer International Publishing Switzerland, 2016.
- [17] T. Vidas, Volatile memory acquisition via warm boot memory survivability, in: 2010 43rd Hawaii International Conference on System Sciences, 2010, pp. 1–6. doi:10.1109/HICSS.2010.439.
- [18] A. Halderman, S. D. Schoen, Heninger, W. Clarkson, Lest we remember: Cold boot attacks on encryption keys, in: USENIX Association 17th USENIX Security 45, 2008.
- [19] T. Heckmann, T. Souvignet, D. Naccache, Electrically conductive adhesives, thermally conductive adhesives and UV adhesives in data extraction forensics, Digital Investigation 21 (2017) 53–64. doi:<http://dx.doi.org/10.1016/j.diin.2017.02.009>. URL <http://www.sciencedirect.com/science/article/pii/S1742287616301347>
- [20] M. E. Baron, The origins of the infinitesimal calculus, Courier Corporation, 1969.
- [21] J. Felba, Chapter 2: Thermally conductive adhesives in electronics, in: M. Alam, C. Bailey (Eds.), Advanced Adhesives in Electronics, Woodhead Publishing Series in Electronic and Optical Materials, Woodhead Publishing, 2011, pp. 15–52. doi:<http://dx.doi.org/10.1533/9780857092892.1.15>. URL <http://www.sciencedirect.com/science/article/pii/B9781845695767500027>
- [22] T. Falat, A. Wymysowski, J. Kolbe, Numerical approach to characterization of thermally conductive adhesives, Microelectronics Reliability 47 (2-3) (2007) 342–346. doi:<http://dx.doi.org/10.1016/j.microrel.2006.02.019>. URL <http://www.sciencedirect.com/science/article/pii/S0026271406000710>
- [23] T. Heckmann, T. Souvignet, S. Lepeer, D. Naccache, Low-temperature low-cost 58 bismuth 42 tin alloy forensic chip re-balling and re-soldering, Digital Investigation 19 (2016) 60–68. doi:<http://dx.doi.org/10.1016/j.diin.2016.10.003>. URL <http://www.sciencedirect.com/science/article/pii/S1742287616301001>
- [24] BlackBerry-Enterprise-Server, Blackberry security technical overview, [online] https://help.blackberry.com/en/bes5-for-exchange/current/sto-pdf/BlackBerry_Enterprise_Server_for_Microsoft_Exchange-Security_Technical_Overview-1330547681607-5.0.4-en.pdf (2014). URL https://help.blackberry.com/en/bes5-for-exchange/current/sto-pdf/BlackBerry_Enterprise_Server_for_Microsoft_Exchange-Security_Technical_Overview-1330547681607-5.0.4-en.pdf